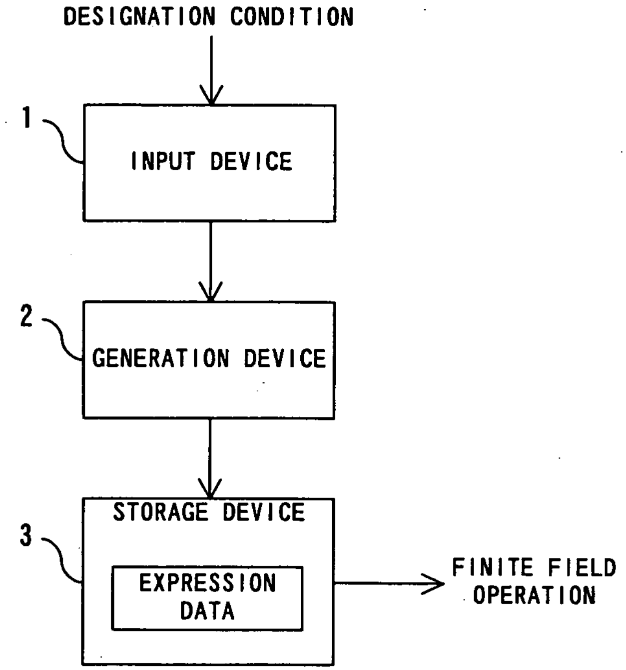

DESIGNATION CONDITION
1
INPUT DEVICE
2
GENERATION DEVICE
3
STORAGE DEVICE
EXPRESSION DATA
FINITE FIELD OPERATION

FIG. 1

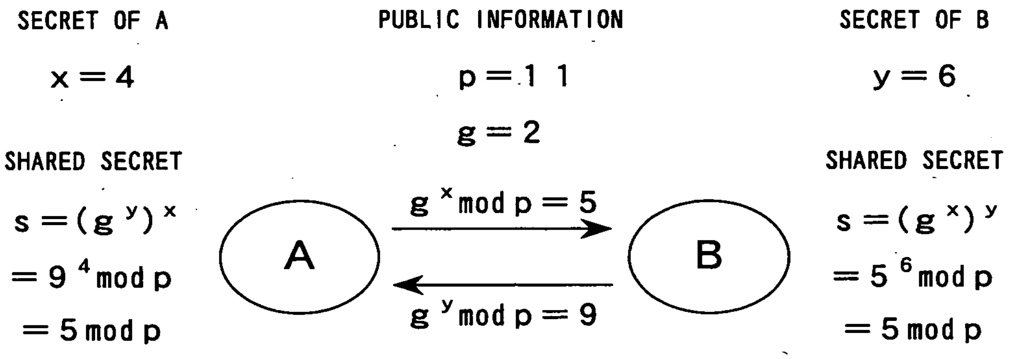

SECRET OF A
$x = 4$
SHARED SECRET
$s = (g^y)^x$
$= 9^4 \bmod p$
$= 5 \bmod p$
PUBLIC INFORMATION
$p = 11$
$g = 2$
$g^x \bmod p = 5$
A
B
$g^y \bmod p = 9$
SECRET OF B
$y = 6$
SHARED SECRET
$s = (g^x)^y$
$= 5^6 \bmod p$
$= 5 \bmod p$

FIG. 2

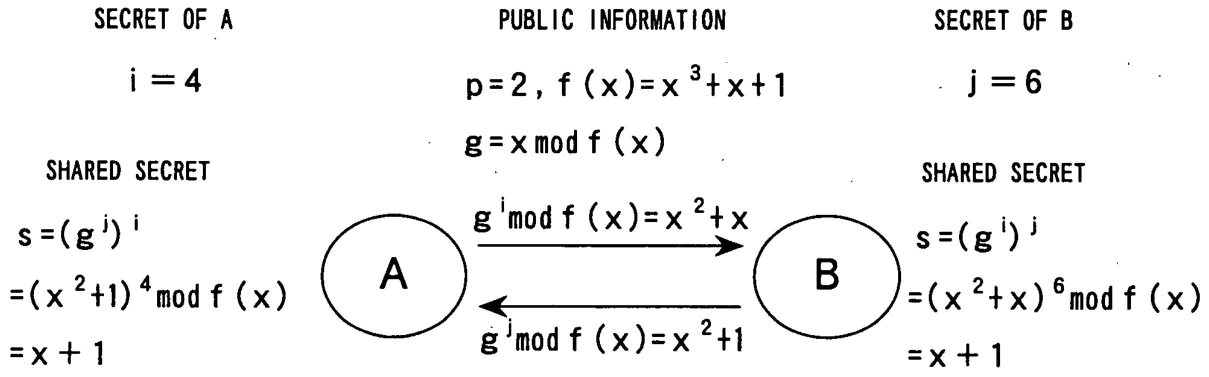
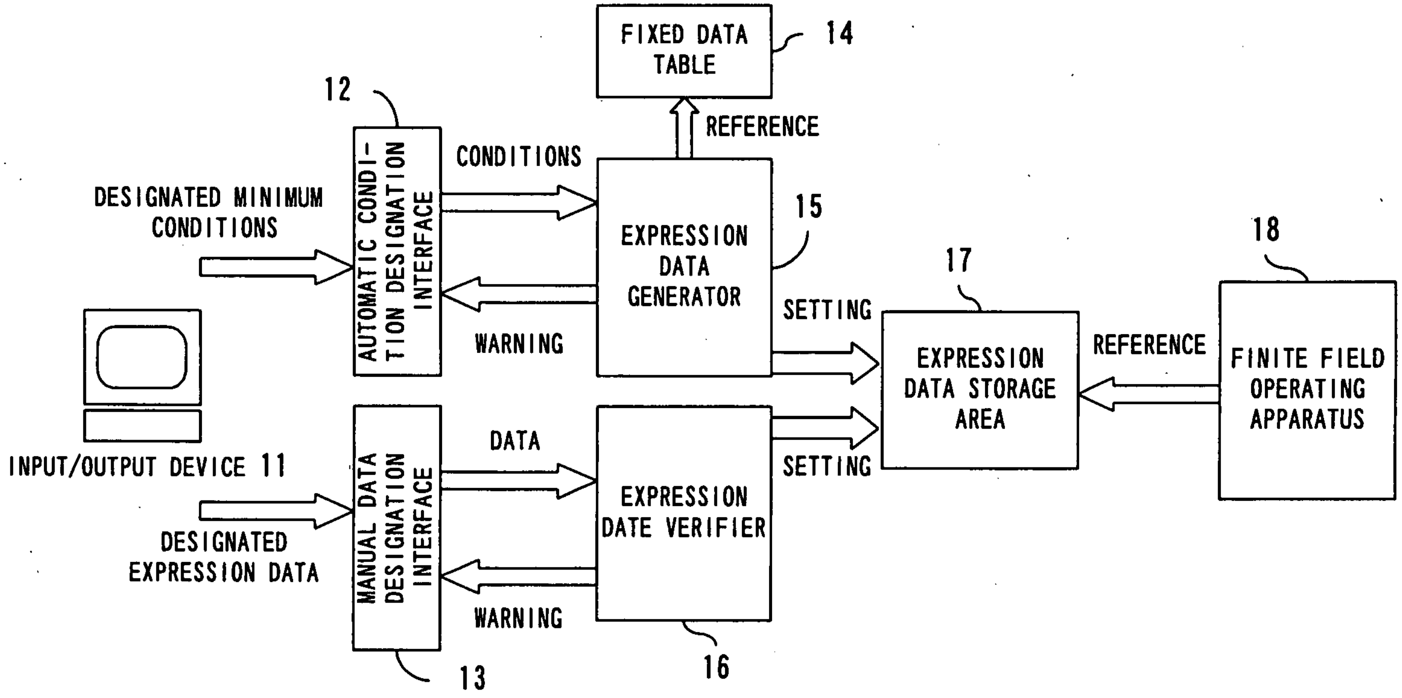

SECRET OF A
$i=4$
SHARED SECRET
$s=(g^{j})^{i}$
$=(x^{2}+1)^{4} \bmod f(x)$
$=x+1$
PUBLIC INFORMATION
$p=2,\ f(x)=x^{3}+x+1$
$g=x \bmod f(x)$
$g^{i} \bmod f(x)=x^{2}+x$
$g^{j} \bmod f(x)=x^{2}+1$
A
B
SECRET OF B
$j=6$
SHARED SECRET
$s=(g^{i})^{j}$
$=(x^{2}+x)^{6} \bmod f(x)$
$=x+1$

FIG. 3


DESIGNATED MINIMUM CONDITIONS
12
AUTOMATIC CONDITION DESIGNATION INTERFACE
CONDITIONS
WARNING
FIXED DATA TABLE
14
REFERENCE
EXPRESSION DATA GENERATOR
15
SETTING
17
EXPRESSION DATA STORAGE AREA
REFERENCE
18
FINITE FIELD OPERATING APPARATUS
INPUT/OUTPUT DEVICE 11
DESIGNATED EXPRESSION DATA
MANUAL DATA DESIGNATION INTERFACE
13
DATA
WARNING
EXPRESSION DATE VERIFIER
16
SETTING

F I G. 4

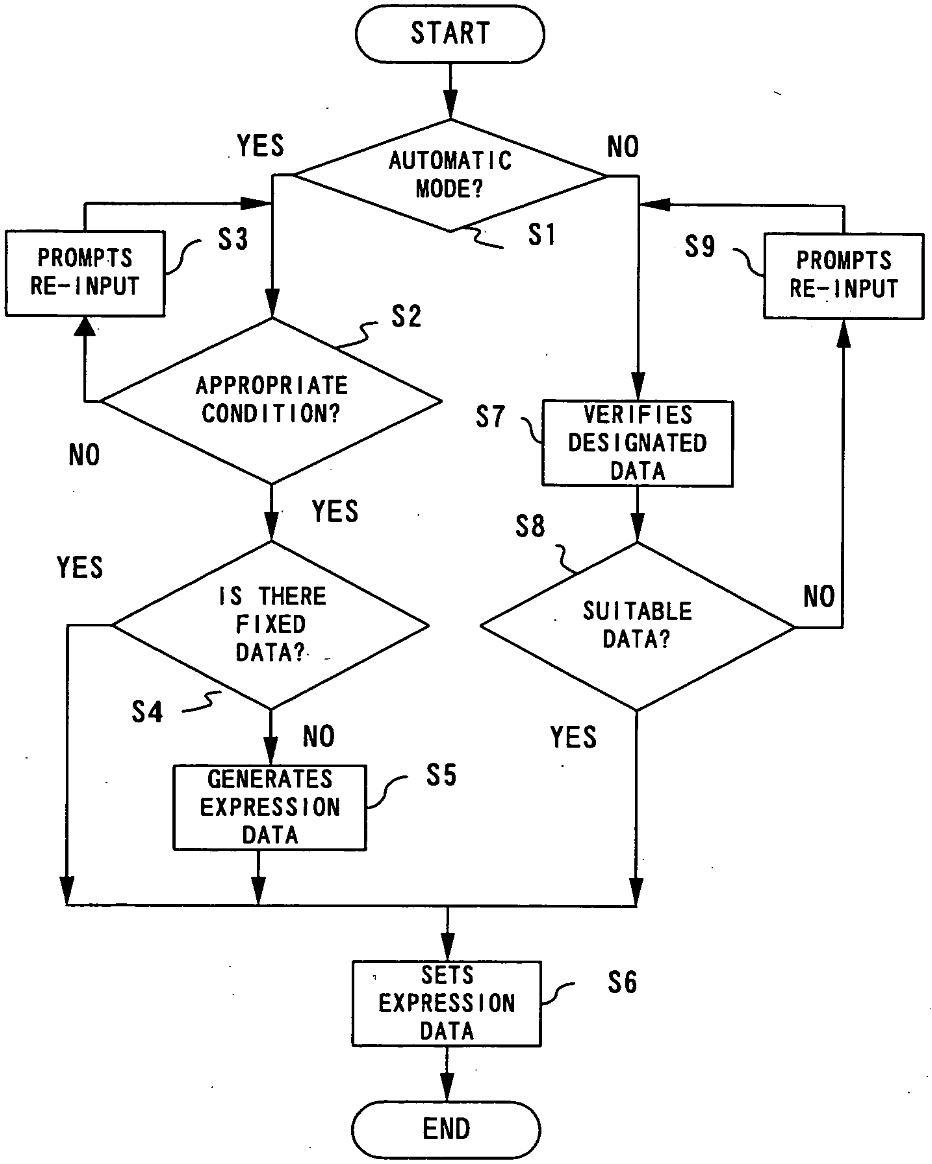
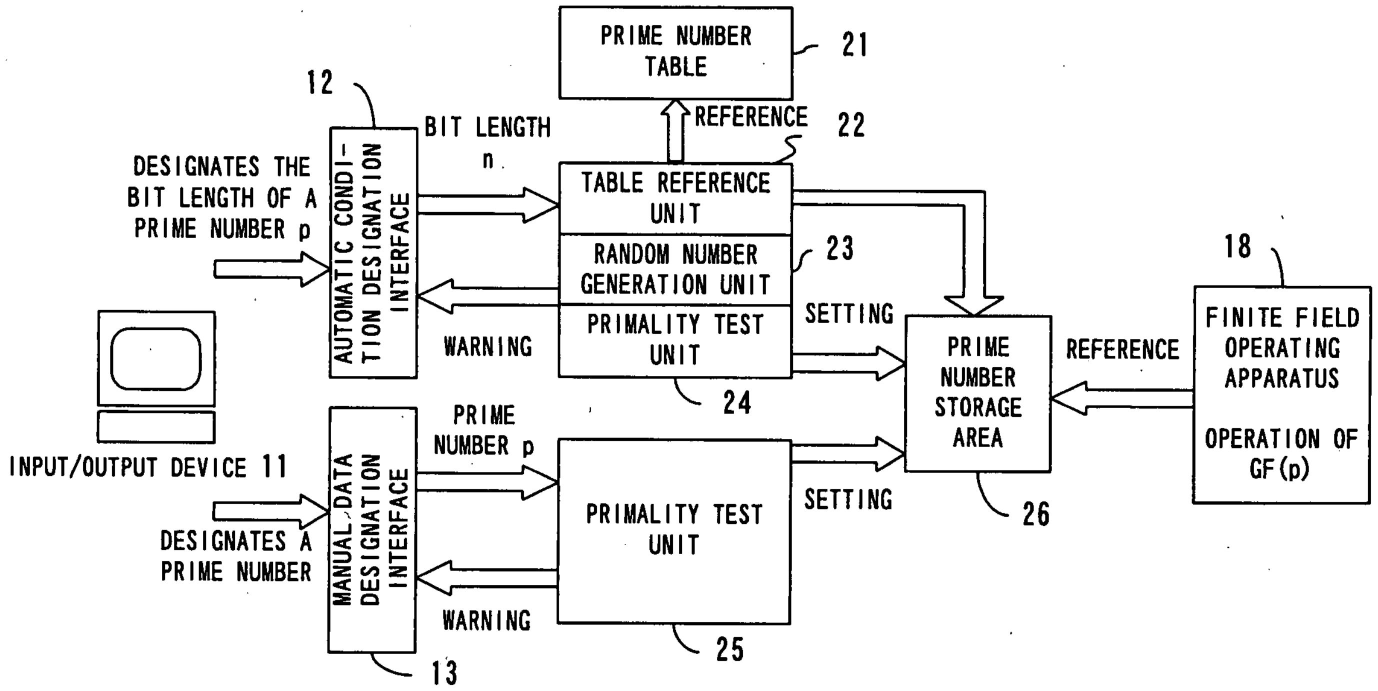


FIG. 5

09503205.021100


PRIME NUMBER TABLE
21
12
BIT LENGTH n
REFERENCE
22
DESIGNATES THE BIT LENGTH OF A PRIME NUMBER p
AUTOMATIC CONDITION DESIGNATION INTERFACE
TABLE REFERENCE UNIT
RANDOM NUMBER GENERATION UNIT
23
18
PRIMALITY TEST UNIT
SETTING
WARNING
PRIME NUMBER STORAGE AREA
REFERENCE
FINITE FIELD OPERATING APPARATUS
OPERATION OF GF(p)
24
INPUT/OUTPUT DEVICE 11
PRIME NUMBER p
MANUAL DATA DESIGNATION INTERFACE
DESIGNATES A PRIME NUMBER
PRIMALITY TEST UNIT
SETTING
26
WARNING
25
13

F I G. 6

BIT LENGTH n	PRIME NUMBER OF n BITS
2	3
3	7
4	11
⋮	⋮

FIG. 7

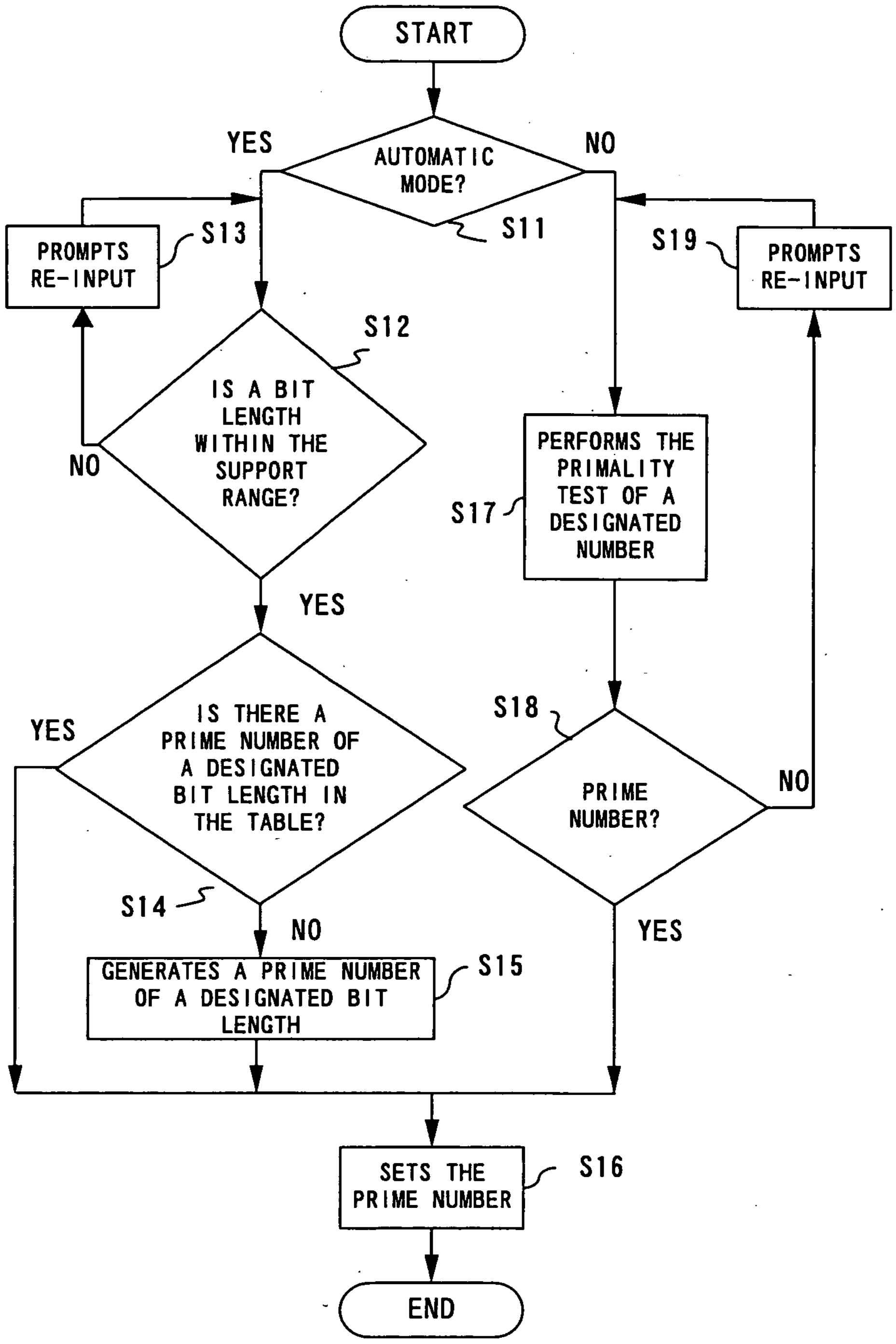
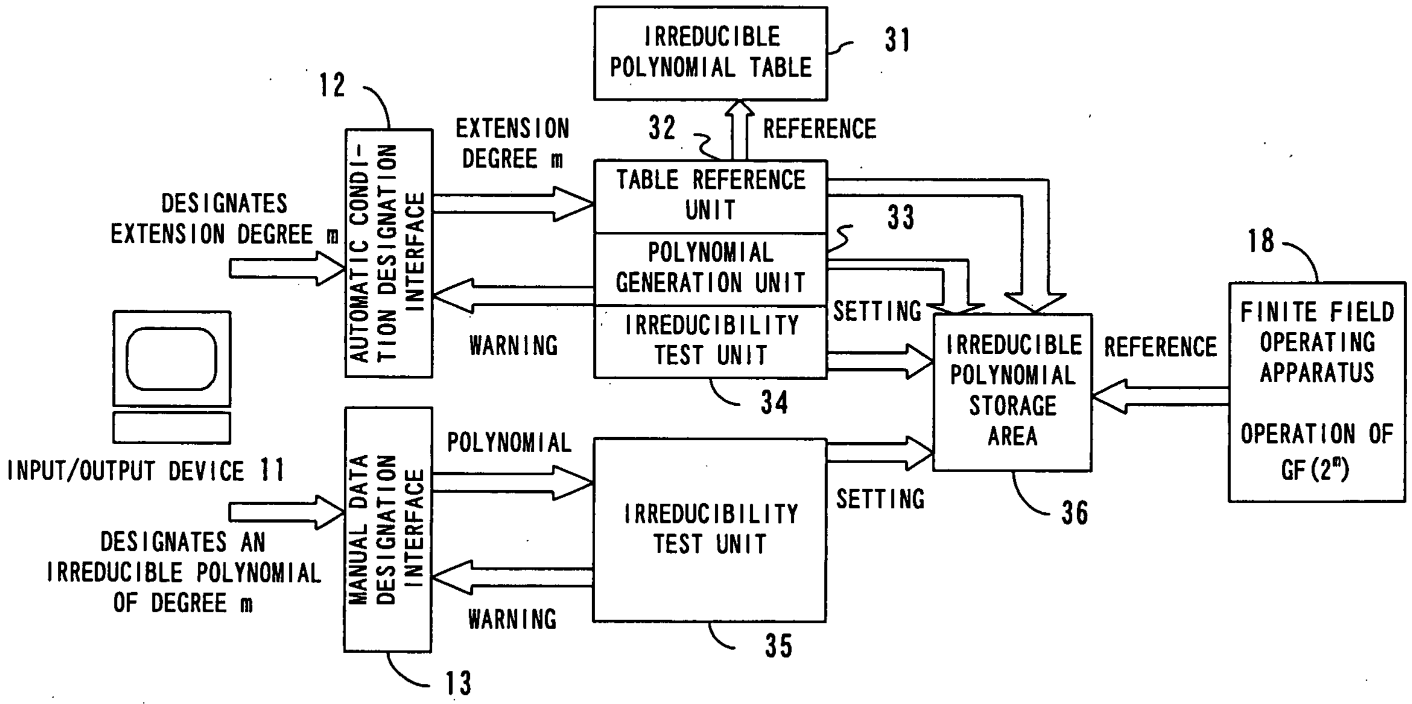

START
AUTOMATIC MODE?
S11
YES
NO
PROMPTS RE-INPUT
S13
S12
IS A BIT LENGTH WITHIN THE SUPPORT RANGE?
NO
YES
IS THERE A PRIME NUMBER OF A DESIGNATED BIT LENGTH IN THE TABLE?
YES
S14
NO
GENERATES A PRIME NUMBER OF A DESIGNATED BIT LENGTH
S15
S19
PROMPTS RE-INPUT
PERFORMS THE PRIMALITY TEST OF A DESIGNATED NUMBER
S17
S18
PRIME NUMBER?
NO
YES
SETS THE PRIME NUMBER
S16
END

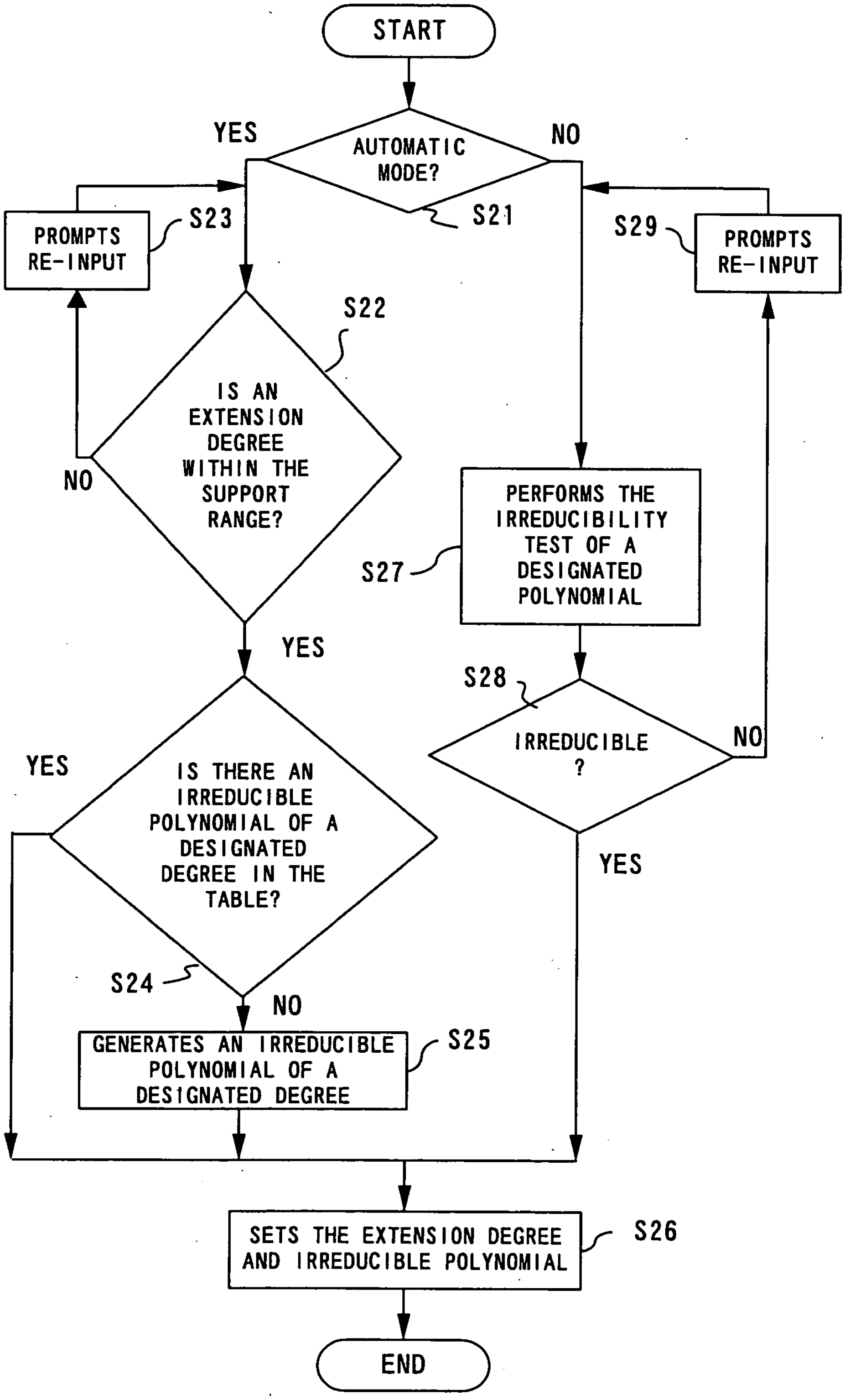
FIG. 8


IRREDUCIBLE POLYNOMIAL TABLE
31
12
EXTENSION DEGREE m
32
REFERENCE
DESIGNATES EXTENSION DEGREE m
AUTOMATIC CONDITION DESIGNATION INTERFACE
TABLE REFERENCE UNIT
33
POLYNOMIAL GENERATION UNIT
18
SETTING
WARNING
IRREDUCIBILITY TEST UNIT
IRREDUCIBLE POLYNOMIAL STORAGE AREA
REFERENCE
FINITE FIELD OPERATING APPARATUS
OPERATION OF GF(2^m)
34
INPUT/OUTPUT DEVICE 11
MANUAL DATA DESIGNATION INTERFACE
POLYNOMIAL
DESIGNATES AN IRREDUCIBLE POLYNOMIAL OF DEGREE m
IRREDUCIBILITY TEST UNIT
SETTING
36
WARNING
35
13

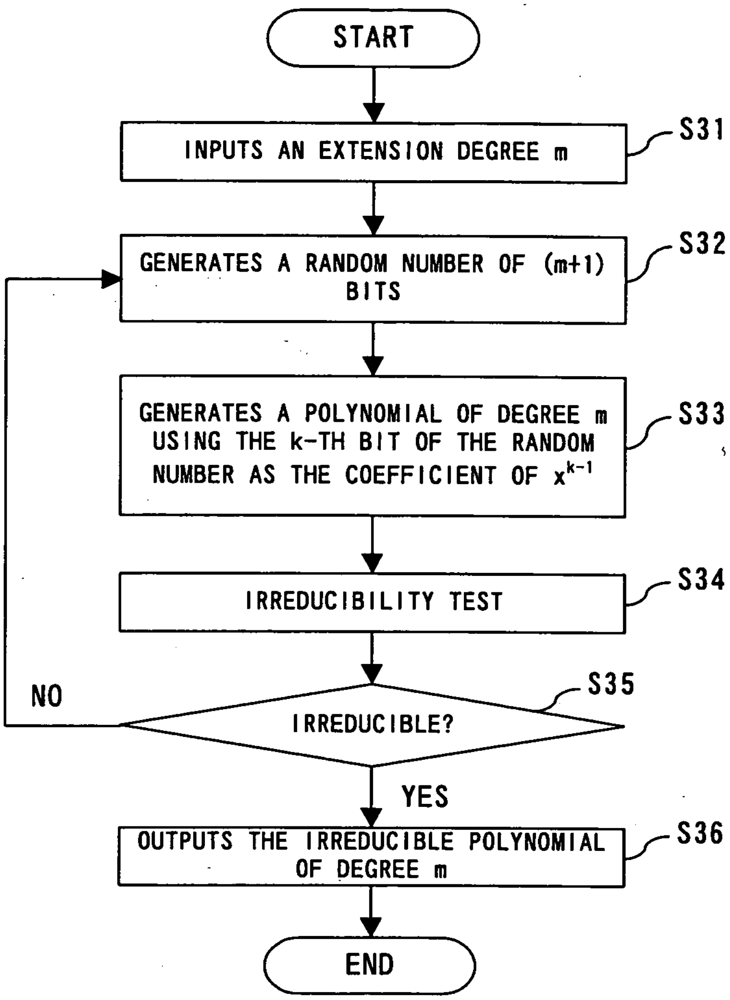
F I G. 9

EXTENSION DEGREE m	IRREDUCIBLE POLYNOMIAL OF DEGREE m
2	x^2+x+1
3	x^3+x+1
4	x^4+x+1
⋮	⋮

FIG. 10


START
AUTOMATIC MODE?
S21
YES
NO
PROMPTS RE-INPUT
S23
S29
PROMPTS RE-INPUT
S22
IS AN EXTENSION DEGREE WITHIN THE SUPPORT RANGE?
NO
YES
PERFORMS THE IRREDUCIBILITY TEST OF A DESIGNATED POLYNOMIAL
S27
S28
IRREDUCIBLE ?
NO
YES
YES
IS THERE AN IRREDUCIBLE POLYNOMIAL OF A DESIGNATED DEGREE IN THE TABLE?
S24
NO
GENERATES AN IRREDUCIBLE POLYNOMIAL OF A DESIGNATED DEGREE
S25
SETS THE EXTENSION DEGREE AND IRREDUCIBLE POLYNOMIAL
S26
END

F I G. 1 1


START
INPUTS AN EXTENSION DEGREE m
S31
GENERATES A RANDOM NUMBER OF (m+1) BITS
S32
GENERATES A POLYNOMIAL OF DEGREE m USING THE k-TH BIT OF THE RANDOM NUMBER AS THE COEFFICIENT OF x^{k-1}
S33
IRREDUCIBILITY TEST
S34
NO
IRREDUCIBLE?
S35
YES
OUTPUTS THE IRREDUCIBLE POLYNOMIAL OF DEGREE m
S36
END

F I G. 12

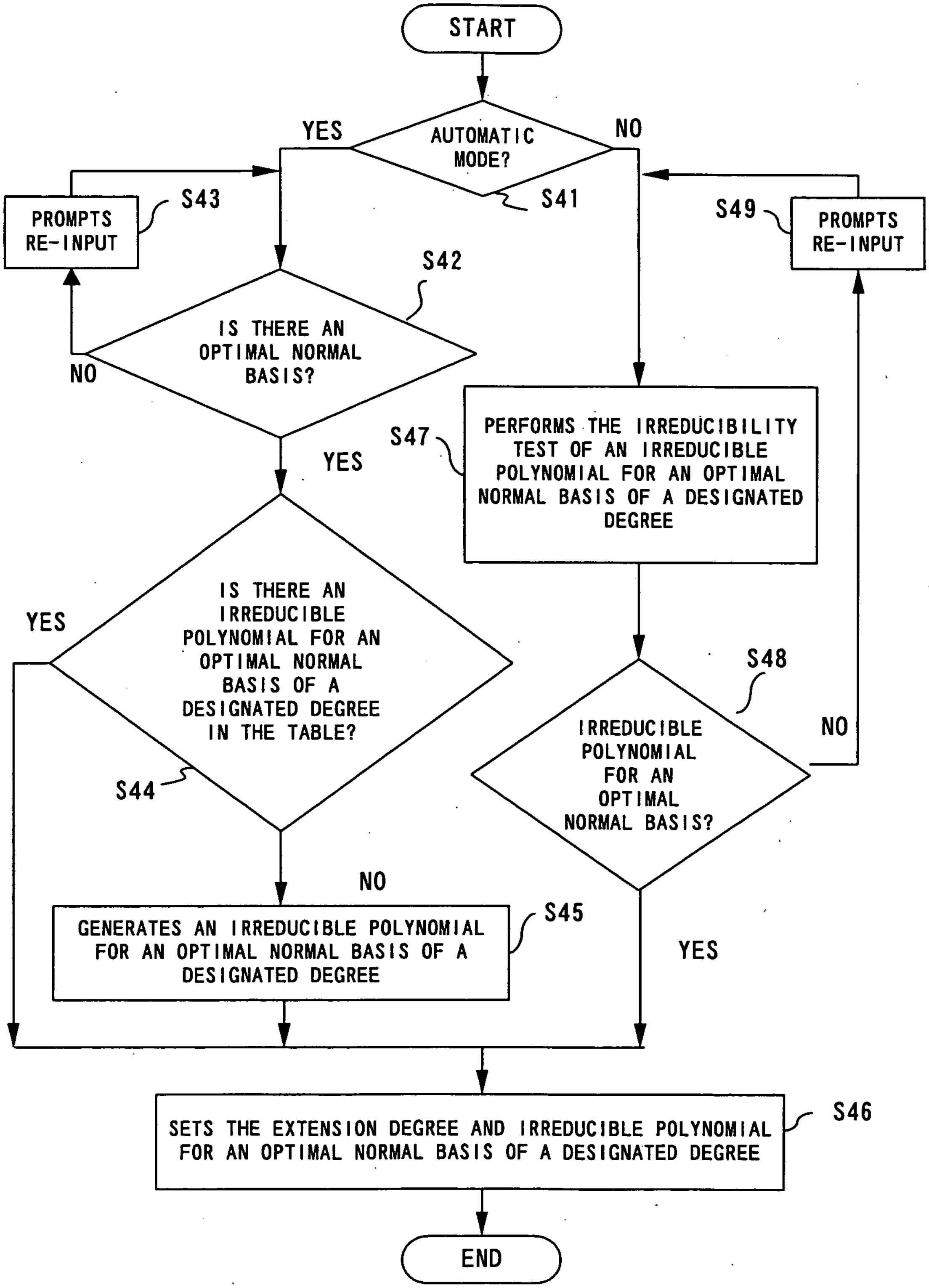

START
AUTOMATIC MODE?
S41
YES
NO
PROMPTS RE-INPUT
S43
S42
IS THERE AN OPTIMAL NORMAL BASIS?
NO
YES
IS THERE AN IRREDUCIBLE POLYNOMIAL FOR AN OPTIMAL NORMAL BASIS OF A DESIGNATED DEGREE IN THE TABLE?
S44
YES
NO
GENERATES AN IRREDUCIBLE POLYNOMIAL FOR AN OPTIMAL NORMAL BASIS OF A DESIGNATED DEGREE
S45
S49
PROMPTS RE-INPUT
S47
PERFORMS THE IRREDUCIBILITY TEST OF AN IRREDUCIBLE POLYNOMIAL FOR AN OPTIMAL NORMAL BASIS OF A DESIGNATED DEGREE
S48
IRREDUCIBLE POLYNOMIAL FOR AN OPTIMAL NORMAL BASIS?
NO
YES
SETS THE EXTENSION DEGREE AND IRREDUCIBLE POLYNOMIAL FOR AN OPTIMAL NORMAL BASIS OF A DESIGNATED DEGREE
S46
END

FIG. 13

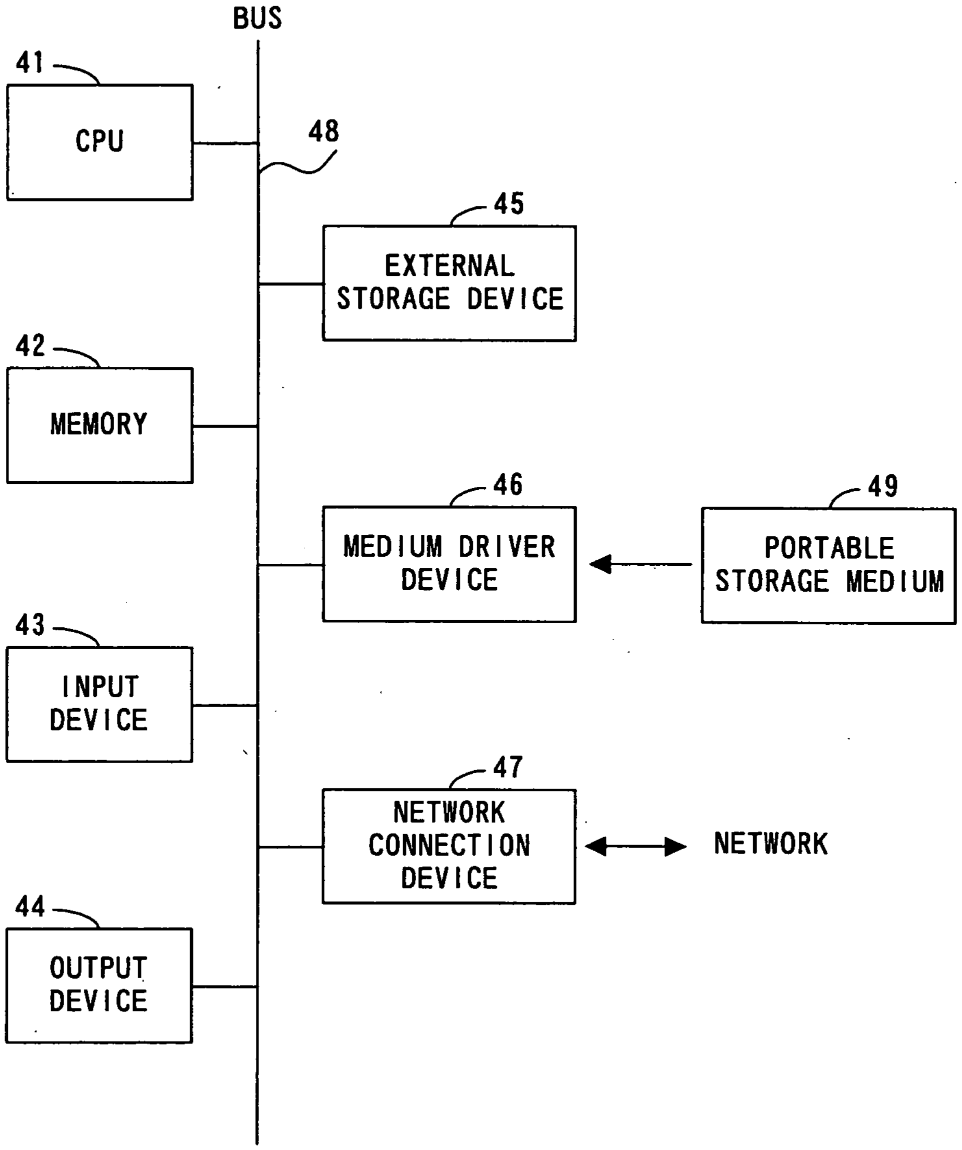
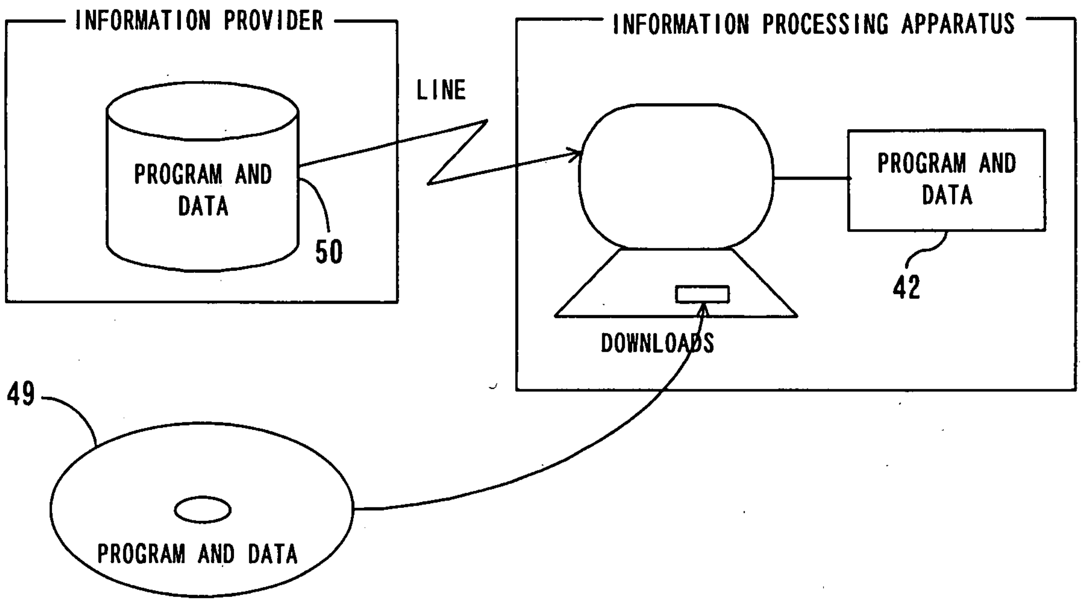

BUS
41
CPU
48
45
EXTERNAL STORAGE DEVICE
42
MEMORY
46
MEDIUM DRIVER DEVICE
49
PORTABLE STORAGE MEDIUM
43
INPUT DEVICE
47
NETWORK CONNECTION DEVICE
NETWORK
44
OUTPUT DEVICE

FIG. 14


INFORMATION PROVIDER
PROGRAM AND DATA
50
LINE
INFORMATION PROCESSING APPARATUS
PROGRAM AND DATA
42
DOWNLOADS
49
PROGRAM AND DATA

F I G. 1 5